Abstract

One of the fundamental problems in commutative algebra and algebraic geometry is to understand the nature of the solution space of a system of multivariate polynomial equations over a field $\Bbbk$, such as real or complex numbers. An important algorithmic tool in this study is the notion of Gröbner bases (Buchberger, 1965). Given a system of polynomial equations, $f_1 = 0, \ldots, f_m = 0$, Gröbner basis is a "canonical" generating set of the ideal generated by $f_1, \ldots, f_m$, that can answer, constructively, many questions in computational ideal theory. It generalizes several concepts of univariate polynomials like resultants to the multivariate case, and answers decisively the ideal membership problem. The dimension of the solution set of an ideal $\mathfrak{a}$ called the affine variety, an important concept in algebraic geometry, is equal to the Krull dimension of the corresponding coordinate ring, $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$. Gröbner bases were first introduced to compute $\Bbbk$-vector space bases of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ and use that to characterize zero-dimensional solution sets. Since then, Gröbner basis techniques have provided a generic algorithmic framework for computations in control theory, cryptography, formal verification, robotics, etc, that involve multivariate polynomials over fields.

The main aim of this thesis is to study problems related to computational ideal theory over Noetherian commutative rings (e.g: the ring of integers, $\mathbb{Z}$, the polynomial ring over a field, $\Bbbk[y_1, \ldots, y_m]$, etc) using the theory of Gröbner bases. These problems surface in many domains including lattice based cryptography, control systems, system-on-chip design, etc. Although, formal and standard techniques are available for polynomial rings over fields, the presence of zero divisors and non units make developing similar techniques for polynomial rings over rings challenging.

Given a polynomial ring over a Noetherian commutative ring, A and an ideal $\mathfrak{a}$ in $A[x_1, \ldots, x_n]$, the first fundamental problem that we study is whether the residue class polynomial ring, $A[x_1, \ldots, x_n]/\mathfrak{a}$ is a free A-module or not. Note that when $A = \Bbbk$, the answer is always 'yes' and the $\Bbbk$-vector space basis of $\Bbbk[x_1, \ldots, x_n]/\mathfrak{a}$ plays an important role in computational ideal theory over fields. In our work, we give a Gröbner basis characterization for $A[x_1, \ldots, x_n]/\mathfrak{a}$ to have a free A-module representation w.r.t. a monomial ordering. For such A-algebras, we

give an algorithm to compute its A-module basis. This extends the Macaulay-Buchberger basis theorem to polynomial rings over Noetherian commutative rings. These results help us develop a theory of border bases in $A[x_1, \ldots, x_n]$ when the residue class polynomial ring is finitely generated. The theory of border bases is handled as two separate cases: (i) $A[x_1, \ldots, x_n]/\mathfrak{a}$ is free and (ii) $A[x_1, \ldots, x_n]/\mathfrak{a}$ has torsion submodules.

For the special case of $A = \mathbb{Z}$, we show how short reduced Gröbner bases and the characterization for a free A-module representation help identify the cases when $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ is isomorphic to $\mathbb{Z}^N$ for some $N \in \mathbb{N}$. Ideals in such $\mathbb{Z}$-algebras are called ideal lattices. These structures are interesting since this means we can use the algebraic structure, $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ as a representation for point lattices and extend all the computationally hard problems in point lattice theory to $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$. Univariate ideal lattices are widely used in lattice based cryptography for they are a more compact representation for lattices than matrices. In this thesis, we give a characterization for multivariate ideal lattices and construct collision resistant hash functions based on them using Gröbner basis techniques. For the construction of hash functions, we define a worst case problem, shortest substitution problem w.r.t. an ideal in $\mathbb{Z}[x_1, \ldots, x_n]$, and establish hardness results for this problem.

Finally, we develop an approach to compute the Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ using Gröbner bases, when A is a Noetherian integral domain. When A is a field, the Krull dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ has several equivalent algorithmic definitions by which it can be computed. But this is not true in the case of arbitrary Noetherian rings. We introduce the notion of combinatorial dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$ and give a Gröbner basis method to compute it for residue class polynomial rings that have a free A-module representation w.r.t. a lexicographic ordering. For such A-algebras, we derive a relation between Krull dimension and combinatorial dimension of $A[x_1, \ldots, x_n]/\mathfrak{a}$. For A-algebras that have a free A-module representation w.r.t. degree compatible monomial orderings, we introduce the concepts of Hilbert function, Hilbert series and Hilbert polynomials and show that Gröbner basis methods can be used to compute these quantities. We then proceed to show that the combinatorial dimension of such A-algebras is equal to the degree of the Hilbert polynomial. This enables us to extend the relation between Krull dimension and combinatorial dimension to A-algebras with a free A-module representation w.r.t. a degree compatible ordering as well.